REMARKS

Favorable reconsideration and allowance of the present application are respectfully requested in view of the following remarks. Claims 1-28 remain pending. Claims 1, 9 and 13 are independent.

ALLOWABLE SUBJECT MATTER

Applicant appreciates that the Examiner considers claims 14-16 and 20-22 define allowable subject matter. *See Final Office Action, page 15, Item 8.*

SCOPE OF CLAIMS NOT ALTERED

Claim 1 is amended merely to address an antecedent basis issue. It is intended that the scope of the claim is not narrowed by the amendment.

§ 102 REJECTION – STEINBERG

Claims 9, 13, 17-19, 23 and 26 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Steinberg et al. (U.S. Patent 6,433,818). *See Final Office Action, Item 3, pages 4-6.* Applicant respectfully traverses.

Independent claim 9 recites, in part "inputting fingerprint data to the digital camera", "checking if the inputted fingerprint data is identical with fingerprint data registered with a fingerprint register of the digital camera" and "automatically initiating a registering of the inputted fingerprint data having a corresponding identifier with the fingerprint register in case no fingerprint data is registered with the fingerprint register." In other words, it is determined whether or not there are any fingerprint data already registered in the fingerprint register. If it is determined that there are no registered fingerprint data, the inputted fingerprint data is automatically registered.

In contrast, when setting up biometric signature data, Steinberg makes no determination regarding there are any preexisting biometric signature data already stored. As illustrated in Figure 7, the biometric signature data is set up in Step 106. *See also Column 5, lines 35-42.* The process of setting up the biometric data is illustrated in Figure 8. Steinberg discloses that in operation, a user enters a predetermined password to instruct the camera to create the biometric data in Step 124. *See also Column 5, lines 55-62.* The user then places either his eye to the view finder or his finger to the shutter button in Step 126 and the camera then records the biometric data in Step 128. The biometric data is then stored in the camera in Step 130. *See also Column 6, lines 5-15.* There is no disclosure whatsoever that the taking of the biometric signature data is contingent upon a determination of whether other biometric signature data already exists.

Indeed, this is reinforced in Column 7, lines 5-51 of Steinberg. Steinberg clearly indicates that an authorized user presents a password / key enabling the camera to acquire and store biometric data. *See Column 7, lines 5-28.* In operation, when a perspective user initiates picture-taking operation, the biometric signature data of the perspective user is analyzed to determine if the user is authorized or not to take pictures. Again, as disclosed in Steinberg, the setting up of the biometric signature data is not dependent upon whether or not there are already stored biometric data.

Clearly, Steinberg cannot teach or suggest the feature of automatically initiating a registering of the inputted fingerprint data in case no fingerprint data is registered as recited in claim 9.

In the Response to Arguments Section, the Examiner indicates that the accepting of the password by the camera can be viewed as the actual initiation because the accepting of the password precedes the placing of the finger of the shutter button. Even if the Examiner's assertion is true, this does not negate the fact that in Steinberg, setting up biometric data is in no way dependent upon whether or not there are preexisting biometric data. Thus, even the Examiner's logic fails.

Independent claim 13 recites, in part, "registering the fingerprint data of the user when it is determined that the digital camera is being used for the first time ever." Thus, claim 13 requires a determination of whether the digital camera is being used for the first time ever as a basis for registering the fingerprint data of the user. Steinberg cannot teach or suggest this feature.

As described above, in order to set up biometrics data, the user must enter a valid keyword or password. Only when the valid password is entered, the camera will then allow the biometrics data to be set. In other words, in Steinberg, whether a valid password is entered or not is the only condition upon which the biometrics data may be set up. The condition of whether or not a valid password has been entered is not the same as determining whether the digital camera itself is being used for the first time.

The Examiner attempts to justify this deficiency by alleging that if a user enters a password, this is an indication that the user is using the camera for the first time.

First, claim states "registering the fingerprint data of the user when it is determined that that the digital camera is being used for the first time ever." In other words, a determination is made as to whether the digital camera is being used for the first time. The claim does not specify a determination of whether or not this particular user is using the camera for the first time. The Examiner is ignoring the plain language of the claim as recited.

More importantly, even given the Examiner's interpretation of claim 13, Steinberg still fails to teach or suggest this feature. As noted, when a biometrics data is to be set up, Steinberg merely requires that a correct password be entered. There is nothing in Steinberg preventing a user from entering the password again to store another biometrics data. For example, a user may have entered his forefinger when setting up his biometrics data initially. He may then wish to change the biometrics data to be based on another of his fingers. Simply put, entering the correct password does not necessarily indicate that the camera is being used for the first time by that particular user. Clearly, the Examiner's logic fails. For at least this reason, independent claim 13 is distinguishable over Steinberg.

Claims 17-19, 23 and 26 depend from independent claim 13 directly or indirectly. Therefore, for at least due to the dependency thereon, these dependent claims are also distinguishable over Steinberg.

The dependent claims are also distinguishable on their own merit. For example, claim 19 recites in part "receiving an instruction from the user when it is determined that the user is a registered user" and "registering a new user to the digital camera when the received instruction specifies registering the new user." In other words, a currently authorized user must instruct registering of a new user.

In contrast, Steinberg merely requires that a correct password be entered. The correct password can be entered by a new user and the biometrics data may be set up for the new user without ever receiving an instruction from a current user to register the new user. Clearly, Steinberg cannot teach or suggest the feature as recited in claim 19.

For at least the above stated reasons, Applicant respectfully requests that the rejection of claims 9, 13, 17-19, 23 and 26 based on Steinberg be withdrawn.

§ 103 REJECTION – STEINBERG

Claim 10 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Steinberg. *See Final Office Action, item 4, pages 6-7.* Applicant respectfully traverses.

It is noted that claim 10 depends from claim 9 and it is shown above that claim 9 is distinguishable over Steinberg. Thus, for at least due to the dependency thereon as well as on its own merit, claim 10 is also distinguishable over Steinberg.

Applicant respectfully requests that the rejection of claim 10 based on Steinberg be withdrawn.

§ 103 REJECTION – STEINBERG, WASULA

Claims 1-2, 4-8, 11, 12, 24, 25 and 27 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Steinberg in view of Wasula et al. (U.S. Publication 2002/0054224). *See final Office Action, Item 5, pages 7-14.* Applicant respectfully traverses.

Independent claim 1 recites, in part, "an authorizer for storing therein an identifier specific to the fingerprint data identified by said comparison circuit" and "a controller for accessing said authorizer to reference the identifier stored in said authorizer and executing the instruction if the instruction is intended the handle a frame of image data associated with the identifier stored in said authorizer." The Examiner readily admits that Steinberg cannot teach or suggest these features. *See final Office Action, page 8, lines 8-15.*

To allegedly correct these deficiencies of Steinberg, the Examiner relies upon Wasula. The Examiner alleges that the profiles as disclosed in Wasula are essentially the same as the specific identifier as recited in the claims. It was demonstrated in the previous reply submitted on November 10, 2005 that the profiles as disclosed in Wasula are merely examples of a collection of instructions, i.e. macros, to be performed by the camera when it is desired to transferred images from the camera to a host computer. The customized profiles contain transferring instructions but this does not imply that they are identifiers specific to a fingerprint data.

In response, the Examiner refers to Figure 3a of Wasula in which an exemplary name of the profile is "John Home Use". The Examiner appears to be under the impression that a name of the collection of instructions in and of itself can be somehow identified with a fingerprint data. First, it is noted that Wasula doesn't even contemplate fingerprint data at all.

Also, this example merely indicates that the profiles may be given arbitrary names for the convenience of the user. The user in creating multiple profiles would likely name each profile to be readily identifiable. However, the name itself has not relevance whatsoever regarding whether it is identified with particular image data.

Also in the Response to Arguments Section, the Examiner asserts that the profiles may be created by a user and access to the profiles may be denied to unauthorized users by employing a password for each profile. Even if this were to be true, this does not prevent other users from entering the correct password and utilizing the profile. In other words, whether or not the profiles themselves are password protected is irrelevant.

It is clear that Wasula in combination with Steinberg cannot teach or suggest the feature of an authorizer for storing therein an identifier specific to the fingerprint data and a controller for accessing the authorizer to reference the identifier stored in the authorizer and executing the instruction if the instruction is intended to handle a frame of image data associated with the identifier stored in the authorizer. For at least the above stated reasons, independent claim 1 is distinguishable over the combination of Steinberg and and Wasula.

Claims 2, 4-8 and 27 depend from independent claim 1 directly or indirectly. Then for at least due to the reasons stated with respect to claim 1, these dependent claims are distinguishable over the combination of Steinberg and Wasula.

The dependent claims are also distinguishable on their own merit. For example, claim 27 recites that the storage of the authorizer is volatile. In the final Office Action, the Examiner alleges that memory 42 illustrated in Figure 2 of Steinberg is equivalent to the authorizer as claimed. Then the logical conclusion is that the memory 42 of Steinberg is volatile, i.e., the memory is erased when the camera is turned off.

However, Steinberg indicates that programming data are stored in memory 42. The programming data is used by the microprocessor to carry out operations of the camera 10. *See Steinberg, Column 3, lines 55-61.* If the memory 42 is volatile as the Examiner suggests, then all programming information would be lost when the camera is powered down. When the camera is powered back up, the camera would be inoperative since the microprocessor would not have access to any programming information. In other words, the camera would be rendered inoperative for its intended purpose. Clearly, claim 27 is distinguishable over the combination of Steinberg and Wasula on its own merit.

Claims 11-12 depend from independent claim 9 and it is demonstrated above that claim 9 is distinguishable over Steinberg. Wasula is relied upon to correct for at least the above noted deficiencies of Steinberg. Therefore, independent claim 9 is distinguishable over the combination of Steinberg and Wasula. Then, for at least due to the dependency thereon, claims 11 and 12 are also distinguishable over the combination of Steinberg and Wasula.

Claims 24 and 25 depend from independent claim 13 and it is demonstrated above that claim 13 is distinguishable over Steinberg. Wasula is not relied upon to correct for at least the above noted deficiencies of Steinberg. Therefore, claim 13 is distinguishable over the combination of Steinberg and Wasula. Claims 24 and 24 are distinguishable over the same combination for at least the reasons stated above with respect to claim 13.

Applicant respectfully requests that the rejection of claims 1, 2, 4-8, 11-12, 24-25 and 27 based on Steinberg and Wasula be withdrawn.

§ 103 REJECTION – STEINBERG, WASULA, KRAMER

Claim 3 stands rejected under 35 USC 103(a) as allegedly being unpatentable over Steinberg and Wasula and in further view of Kramer et al. (US Publication 2001/0043728). *See Office Action item 7.* Applicant respectfully traverses.

It is noted that claim 3 depends on claim 1 and it is above that claim 1 is distinguishable over the combination of Steinberg and Wasula. Kramer has not been and cannot be relied upon to correct for at least the above noted deficiencies of Steinberg and Wasula. Therefore, claim 1 is distinguishable over the combination of Steinberg, Wasula and Kramer.

For at least due to the dependency thereon as well as on its own merit, claim 3 is also distinguishable over the combination of Steinberg, Wasula and Kramer.

Applicant respectfully requests that the rejection of claim 3 based on Steinberg, Wasula and Kramer be withdrawn.

§ 103 REJECTION – STEINBERG, SATOH

Claim 28 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Steinberg in view of Satoh (U.S. Publication 2001/0002933). *See final Office Action, Item 7, page 14.* Applicant respectfully traverses.

Claim 28 depends from independent claim 13 and it is demonstrated above that claim 13 is distinguishable over Steinberg. Satoh is not relied upon to correct for at least the above-noted deficiencies of Steinberg. Therefore, claim 13 is distinguishable over the combination of Steinberg and Satoh. Due to the dependency thereon, claim 28 is also distinguishable over Steinberg and Satoh.

Further, claim 28 is distinguishable on its own merits. Claim 28 recites, in part "determining whether there are no registered users." The Examiner alleges that Figure 2 of Satoh teaches this feature. However, Figure 2 of Satoh merely indicates that a current inputted fingerprint data is registered or not. There is no indication that suggests determining whether or not there are any registered fingerprint data at all. Clearly, claim 28 is distinguishable on its owner merit.

Applicant respectfully requests that the rejection of claim 28 based on Steinberg and Satoh be withdrawn.

CONCLUSION

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the present application is in condition for allowance. Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact Hyung Sohn (Reg. No. 44,346), to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH &, BIRCH, LLP

By: ______________________
D. Richard Anderson
Reg. No. 40,439

HNS
DRA/HNS/kj

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000